Appendix N
System Safety Issue: System Evaluation Considerations

N–1. Overview of system safety

Army policy requires that system safety be applied and tailored to all Army systems throughout their life cycle and that safety and health verifications/evaluation be an integral part of the system safety effort. One of the most important aspects of testing is verification of the elimination or control of safety and health hazards. Developmental testing provides determinations of personnel and equipment hazards inherent in the system and associated operation and maintenance hazards, with special attention given to verifying the adequacy of safety and warning devices and other measures employed to control hazards.

N–2. Safety evaluation

Within ATEC, the developmental testers (DTC) serve as the Army's system safety verifier. In this capacity, DTC provides both the Safety Release and the Safety Confirmation.

N–3. Safety Release

The Safety Release is prepared by DTC and provided to the testing organization prior to any testing using soldiers. See chapter 6 for details.

N–4. Safety Confirmation

AR 385–16 requires that a Safety Confirmation be prepared at the end of each phase of the acquisition process and at major decision points. HQ, DTC is responsible for providing the Safety Confirmation for all systems. The Safety Confirmation is prepared and provided to the system evaluator and is attached to the SER as an appendix. The Safety Confirmation will also be provided to the PM, the AMC Safety Office, U.S. Army Safety Center, TRADOC Safety Office, and the MATDEV or PM-supporting Safety Office to support system materiel release. The Safety Confirmation will—

a. Indicate whether the system is completely safe for operation or identify hazards that are not adequately controlled using MIL–STD 882 and AR 385–16 for classification of the hazards.

b. List any technical or operational limitations or precautions.

c. Highlight any safety problems that require further investigation and testing.

N–5. Hazard analysis

a. Hazard analyses are the heart of the system safety evaluation and provide the preparer of the SAR, Safety Release, and Safety Confirmation with a wealth of information. The types of analyses that are performed must be stated in section 4, Safety Engineering of the System Assessment Report.

b. From the beginning, a system must be designed to eliminate or control all potential and actual safety and health hazards. These hazards will be identified in accordance with hazard evaluation techniques and these techniques result in the various hazard analysis documents. The following documents reflect hazard evaluation techniques:

(1) The preliminary hazard analysis is an inductive process that should be conducted early in the design phase of the system life cycle to identify in broad terms the potential hazards associated with the proposed operational concept. The preliminary hazard analysis is prepared by the PM or contractor. It reflects the initial risk assessment of a system and identifies safety critical areas, evaluates hazards, and identifies the safety design criteria to be used.

(2) A System Hazard Analysis (SHA) is submitted by the contractor in accordance with the requirements of the contract data requirements list. It is a systematic assessment of real and potential hazards associated with possible subsystem failure. It identifies hazards and then directs design efforts toward the elimination or control of the hazard. The SHA indicates the hazard severity and the hazard probability levels as established by MIL STD–882.

(3) The Subsystem Hazard Analysis (SSHA) Report is prepared by the PM or contractor. This report identifies hazards associated with component failure modes and functional relationships of components and equipment comprising each subsystem. The SSHA is an inductive process that, in effect, is an expansion of, with increased complexity over, the SHA. It normally occurs during the design phase; however, it can be used during operation as an investigation to establish cause and effect relationships and probabilities.

(4) The Operating and Support Hazard Analysis Report is prepared by the PM or contractor. This report identifies hazards and determines safety requirements for personnel, procedures, and equipment during production, testing, installation, training, escape, and operations. It, too, provides information that can be used in preparing the Safety Release and Safety Confirmation. The Operating and Support Hazard Analysis is normally conducted on all identified hazards involving man/machine interfaces. It helps ensure that corrective or preventive measures will be taken to minimize the possibility that any human error procedure will result in injury or system damage.

c. The Preliminary Hazard Analysis/List is prepared by the PM. It involves making a study during concept or early development of a system to determine the hazards that could be present during operational use.

d. The Software Hazard Analysis should cover the areas reflected at table N–1 as relating to the Safety Release. ITOP 1–1–056, Software Testing, describes the software testing procedures.

e. The Safety Release is a formal document issued by HQ, DTC to the operational tester or other user before any hands-on training, use, or maintenance by soldiers. Copies of the Safety Release are also issued to the system evaluators, combat developers, and PMs. Operational testing, including pretest system training, and DT involving borrowed soldiers will not begin until the test agency, the trainer, and the commander who is providing the test soldiers have received a Safety Release. DTC does not provide the Safety Release for systems developed by the Medical Command (MEDCOM) or for those non-tactical C4/IT systems assigned to CECOM by the HQDA (CIO/G–6) or AMC.

f. The Safety Release indicates the system is safe for use and maintenance during the specified test by typical user troops and describes the specific hazards of the system based on test results, inspections, and system safety analyses. Operational limits and precautions are also included.

g. The requirement for a Safety Release also applies to testing of new or innovative procedures (doctrine and tactics) for the use of materiel that has been type classified. Safety Releases are not required for use of standard equipment in the normal prescribed manner.

h. A Conditional Safety Release is issued when further safety data are pending or operational restrictions are required and restricts certain aspects of the test (for example, a restriction on range fan area until all range safety tests are completed). A Limited Safety Release is issued on one particular system (prototype, model, modification, and software revision) or for one particular test.

i. The tester uses the information contained in the Safety Release to integrate safety into test controls and procedures and to determine if the test objectives can be met within these limits.

j. When unusual health hazards exist, The Surgeon General reviews or participates in preparation of Safety Releases to ensure safety of soldiers during operational testing.

k. The Safety Release is developed at least 60 days prior to pretest training and all types of OT and DT that expose soldiers to training and testing activities involving the research, development, operation, maintenance, repair, or support of operational and training materiel. This requires that pertinent data (for example, results of safety testing and hazard classification) be provided to the Safety Release authority in sufficient time to perform this testing or determine if additional testing is required.

l. The Safety Release format is reflected in AR 385–16.

N–6. Safety requirements

The Human Systems Integration (HSI) portion of the ORD contains the system safety requirements. The essential features needed must be clearly stated so that the technical parameters provide the necessary data to verify/address system safety. The Critical System Characteristics should contain a clear requirement for safety parameters.

a. Prior to MS B, the MATDEV charters the System Safety Working-level IPT (SS WIPT). This group tailors the safety documents to the requirements of the system being developed. This is done through a variety of documents that are sources of information during preparation of the Safety Release.

(1) *System Safety Management Plan (SSMP).* Prepared by the MATDEV, the SSMP is a description of planned methods to be used by the Government in monitoring the contractor's system safety program. It should be reviewed to ensure that ATEC is provided an opportunity to review the requirements and program documents; that the milestone schedule identifies the timely issuance of the System Assessment Report to DTC; and that DTC is provided the results of contractor testing. It identifies system safety management issues and is incorporated as part of the Acquisition Strategy for all systems.

(2) *System Safety Program Plan (SSPP).* The MATDEV will ensure that the contractor prepares and updates a System Safety Program Plan (SSPP). The Safety Verification section should be reviewed to determine the adequacy of procedures for feedback of test information for review and analysis, and the adequacy of procedures established by the contractor's safety organization to ensure safe conduct of all tests. This plan is a description of the contractor's methods to implement the tailored requirements of MIL STD 882, including organizational responsibilities, resources, milestones, depth of effort, and integration with other program engineering and management activities as well as those of related system.

(3) *Health Hazard Assessment Report (HHAR).* The HHAR is prepared by the U.S. Army Center for Health Promotion and Preventive Medicine (CHPPM) at the request of the PM for those systems that require medical advice or assistance for the developmental evaluation of health hazards.

(4) *Safety Assessment Report (SAR).* The MATDEV prepares the SAR or obtains it from the contractor, and provides it to DTC. DTC will not accept a SAR as official unless it has been approved by the MATDEV's supporting safety office. The SAR references the HHAR and includes information on health hazards. It is a formal summary of the safety data collected during the design and development of the system. The MATDEV summarizes the hazard potential of the item, provides a risk assessment, and recommends procedures or other corrective actions to reduce these hazards to an acceptable level. This is a key source of data for the Safety Release. The SAR is updated when changes are made that impact safety.

(5) *System Safety Risk Assessment (SSRA).* The SSRA provides a comprehensive evaluation of the safety risk being assumed for the system under consideration at the MDR. This document is prepared by the MATDEV and supports the decision for accepting residual hazards.

b. Risk assessment criteria contained in MIL–STD–882 is used to assess risks in Army systems and facilities. Based on these criteria, risks will be categorized in a three-tiered hierarchy that is tailored to the individual system requirements and which is applicable to the individual program decision authority structure. Table N–1 provides the hazard probability categories as reflected in MIL–STD–882.

c. The model for risk acceptance authority is reflected in MIL–STD–882. This model can be used for any program if appropriate. Should program requirements dictate a different decision authority, an appropriate matrix is developed by the MATDEV. The recommended matrix will be submitted for approval (as part of the Acquisition Strategy) to the AAE or designated authority. The risk acceptance hierarchy is to be published and updated as required in the appropriate SSMP.

d. In order to obtain safety related data, testing must be completed that is safety specific (for example, noxious fumes or toxic gases, operation at the boundary of the operating environment, and software overload tests). Safety representatives will provide specific software conditions to test for and to be included in the formal test plans and procedures. Most safety related data are obtained during conduct of performance and endurance tests. Therefore, while safety specific tests can be conducted early in the program to provide information for a Safety Release, the information reflected in the test report and Safety Confirmation addresses all testing.

e. MIL–STD–882 provides uniform requirements for developing and implementing a system safety program of sufficient comprehensiveness to identify the hazards of a system and to ensure that adequate measures are taken to eliminate or control the hazards.

f. The Safety Confirmation is based on data from specific safety and health tests performed on hazardous devices, components, or by-products to determine the nature and extent of hazards presented by the materiel. Particular attention is given to identifying and assessing special safety and health hazards presented by radioactive materials, radio frequency emitters, toxic gases, laser devices, toxic and carcinogenic materials, gaseous emissions, blast overpressure, and harmful noise sources.

Table N–1
Safety verification process—hazard probability categories (MIL–STD–882)

	HAZARD PROBABILITY				
	FREQUENT	REASONABLY PROBABLE	OCCASIONAL	REMOTE	IMPROBABLE
SPECIFIC INDIVIDUAL ITEM	Likely to occur frequently	Will occur several times in life of the item	Likely to occur sometime in the life of item	Unlikely but possible to occur in the life of item	So unlikely it can be assumed the occurrence may not be experienced
FLEET OR INVENTORY	Continuously experienced	Will occur frequently	Will occur several times	Unlikely but can reasonably be expected	Unlikely to occur but possible
	HAZARD SEVERITY				
Catastrophic I. May cause death or loss of system	HIGH	HIGH	HIGH	HIGH	MEDIUM
CRITICAL II. May cause severe injury, severe occupational illness, or major system damage	HIGH	HIGH	HIGH	MEDIUM	LOW
MARGINAL III. May cause minor injury, minor occupational illness or minor system damage	HIGH	MEDIUM	MEDIUM	LOW	LOW
NEGLIGIBLE IV. May cause less than minor injury, occupational illness or system damage	MEDIUM	LOW	LOW	LOW	LOW